

**Intrusion
Prevention
Tools for
Defense
In-Depth**

**SANS WhatWorks
in Internet Security**

**TippingPoint
at Discovery
Communications**

2005

TippingPoint at Discovery Communications



About Discovery Communications

Discovery Communications Inc. is the leading global real-world media and entertainment company. Discovery has grown from its core property, the Discovery Channel, first launched in the United States in 1985, to current global operations in more than 160 countries and territories with 1.3 billion cumulative subscribers.

DCI's over 90 networks of distinctive programming represent 25 network entertainment brands including TLC, Animal Planet, Travel Channel, Discovery Health Channel, Discovery Kids, Discovery Times Channel, The Science Channel, Military Channel, Discovery Home Channel, Discovery en Español, Discovery Kids En Español, Discovery HD Theater, FitTV, Discovery Travel & Living (Viajar y Vivir), Discovery Home & Health and Discovery Real Time. DCI's other properties consist of Discovery Education and Discovery Commerce, which operates 120 Discovery Channel Stores.

DCI also distributes BBC America in the United States. DCI's ownership consists of four shareholders: Discovery Holding Company (NASDAQ: DISCA, DISCB), Cox Communications, Inc., Advance/Newhouse Communications and John S. Hendricks, the company's Founder and Chairman.

About Chris Mula

Chris Mula is the IT Security Program Manager at Discovery Communications. He evaluates, recommends, and implements security products, policies, and procedures and standards. He began his IT career as a board designer at Adaptec, and went on to become a system administrator. Then he went into security, working on HIPAA implementation and other contract work before joining Discovery Communications.

SANS Summary

Discovery Communications needed a way to protect its infrastructure and servers against the inherent threats to which a company with a global and mobile workforce of 5,000 staff is susceptible. New variants of malicious software that were undetectable by antivirus tools presented serious problems and risks. The tool they implemented blocked 20,000 to 25,000 individual infection attempts within the first hour and helped business by reducing downtime and avoiding crippling infections.

~~~~~

## *Interview*

### **Q. What led you to look for an intrusion prevention system?**

A. We have a highly mobile and global workforce that includes approximately 3,000 employees with laptops. If there is a virus or other security threat out there, they are most likely going to encounter it. We want to take every possible step to protect our infrastructure and its encounter it. We want to take every possible step to protect our infrastructure and its servers. We needed a solution to protect against what is being brought back every time someone reconnects to our network.

**“..An industry report on IPS systems rated TippingPoint highly.”**

Many of the problems we encounter are new variants of malicious software that antivirus tools are not detecting. In fact, numerous times I have had to send files to the AV companies documenting new variants they had never seen.

### **Q. How did you look for a way to prevent those infections?**

A. We first went down the IDS road to see whether we could we mitigate problems using that technology. We found that it really is not a viable solution.

Then I started looking at application firewalls. But they did not meet our needs. We were trying to protect against problems introduced by our mobile users. An additional reason we could not use firewalls is that they do not look deep enough into the packets. We needed to look at deep packet inspection.

We put out an RFP with requirements for IPS and received seven responses and I met with each of the vendors.

### **Q. What were the key criteria you decided were most important?**

A. We were looking for a hardware solution rather than software, although several hardware solutions had throughput issues. I had vendors telling me that a gig box can push a gig, and we all know that is not the case.

Based on those meetings and discussions with business partners and recommendations from colleagues, I decided to narrow the field and I brought in two products. However,

---

*\*\*To hear Chris Mula expand on the answers, view his presentation slides, and listen to his answers to many more detailed questions asked by other users from around the world, visit the [SANS WebCast Archive](#).*

our network team would not certify either one of them. Both failed miserably on throughput and both had false positives that they could not live with.

After that test, I discovered an industry report on intrusion prevention systems that listed other vendors, particularly TippingPoint, that they rated highly. When the network team said the project would be scrapped if we did not find something that had better throughput and fewer false positives, I called TippingPoint. Within a week the device was in place.

**Q. Did that device pass the network guys' tests?**

A. The network guys loved the TippingPoint appliance. The throughput of the box was 100 megs over the advertised throughput. So they were happy on throughput. As much as they tried to get false positives, they could not so they were also happy about that.

**Q. Were there any requirements that were specific to the media and entertainment industry?**

A. Not really. Throughput (obviously) and false positives were the most important requirements.

**Q. Where did you deploy the technology?**

A. We put one in every regional office domestically and we are expanding internationally.

**Q. What level of senior management approval did you get?**

A. I had to go to the Senior Vice President of Global Infrastructure and Operations. I showed him the number of virus outbreaks and the downtime per user. That included hours that users could not do their work, hours required from desktop engineering, hours required from customer support staff, and hours from people going out to fix each system. It added up to four to five hours per user per outbreak. If we can get them blocked, we can reduce the number substantially.

We also had data on the scale of Blaster-caused problems. We sat down with the parties infected, talked with them about the cleanup time, and picked conservative estimates of the losses. I do not think the numbers alone sold the product. We showed that it would help the business by reducing downtime and avoiding crippling infections. They had experienced Blaster and Slammer -- users cut off from other users and business partners were real financial problems. Everybody had been affected by Nimda or Sasser or Code Red or Melissa. They had all felt the impact.

**“We showed that it would help the business by reducing downtime and avoiding crippling infections.”**

**Q. How do you know it actually works?**

A. We saw it working with Zotob. The antivirus scanners were not picking it up. TippingPoint blocked it. Honestly, if we did not have the TippingPoint in place, we probably would have had a large number of infections. As it was, we had fewer than 100. Our TippingPoint appliance blocked 20,000 to 25,000 individual infection attempts within the first hour.

**Q. Why was it that large?**

A. Because laptops were brought in and they infected their neighbors, but the TippingPoint stopped infections from spreading between offices.

**Q. Any more proof it works?**

A. Yes. We saw the Day Zero virus attack. The antivirus system did not catch it. The only way we knew we had it and what it was trying to do was that our TippingPoint systems showed us.

**Q. What was the deployment process like?**

A. We racked it, put it online and adjusted it. It took less than 30 minutes. The total time per office was a couple hours because we set up our own layer-two fallback to avoid stopping the flow of data. That layer-three work took longer than it took to configure the TippingPoint device.

**Q. What level of manpower does it require and how much training did your staff need?**

A. Training took a couple of days and the total manpower effort is less than one full-time employee.

**“TippingPoint technical support has been a true pleasure to deal with.”**

**Q. What problems arose and how did TippingPoint respond?**

A. We had one NIC card problem. It was very basic. The great thing about this whole engagement is that the TippingPoint people are so on top of it. They provided a replacement unit within 24 hours.

TippingPoint technical support has been a true pleasure to deal with. I can think of many other technology companies where calling tech support was a nightmare. If you call TippingPoint they will take care of it. It has been amazing.

**Q. Did you consider a host-based intrusion prevention alternative?**

A. Yes. But we saw that configuring it worldwide would take much more time than the network-based solution. In the future, everyone will do both network- and host-based intrusion prevention because the virus writers are getting smarter and their attack methods are continuing to grow in sophistication.

**“It has been a great solution and has really helped us ensure the security of our infrastructure.”**

**Q. Are there other technologies you see as critical in a comprehensive protection suite?**

A. Yes. Application security. If someone can get into the application -- that is where the nightmare scenario happens.

**Q. Back to TippingPoint, were there any problems with false positives?**

A. I never saw one. We did see something that looked like a port scan, but it turned out to be a P2P client. You could call it a false positive, but it showed us something we wanted to fix.

**Q. Do you use the IPS for any compliance or audits?**

A. No.

**Q. Any features you would like to see added?**

A. Yes. I would like to see the ability to configure the system to recognize a foreign laptop so that we will know when an "outsider" is on the network.

I would also like to see more logging on the IDS side -- sometimes I need to go back and see what happened.

**Q. What is your bottom line on TippingPoint?**

A. It has been a great solution and has really helped us ensure the security of our infrastructure. Discovery is committed to quality in all that we do -- from programming to IT infrastructure and security.

## SANS Bottom Line

1. Good throughput and no false positives.
2. Deployment took less than 30 minutes.
3. Technical support was "amazing."
4. Helped the business by reducing downtime and avoiding crippling infections.

For more information on TippingPoint  
Visit [www.tippingpoint.com](http://www.tippingpoint.com) or  
Call 1-888 TRUE IPS (+1 888 878 3477)